# подъем ~~упавшей~~ рухнувшей NT

крис касперски ака мыщъх, no-email

**операционные системы семейства NT очень надежны и "сами по себе" падают крайне редко. обычно систему роняют кривые программы, вирусы и непродуманные действия пользователя. как поднять упавшую NT и вернуть все свои данные? без паники! сейчас мыщъх расскажет и покажет!**

## *введение*

Для специалиста слова "*NT/W2K/XP не грузится*" не значат ровным счетом **ничего**. Мог сломаться жесткий диск, пострадать файловая система, разрушиться таблица разделов, слететь первичный/вторичный загрузчик, навернуться реестр, исчезнуть файл ntldr, boot.ini, заглючить драйвер и т. д.

Прежде чем начинать действовать, необходимо произвести первичную диагностику проблемы, тщательно обдумывая каждое свое действие. Один неверный шаг может загубить гигабайты данных, значительно усложняя восстановление или даже делая его практически невозможным.

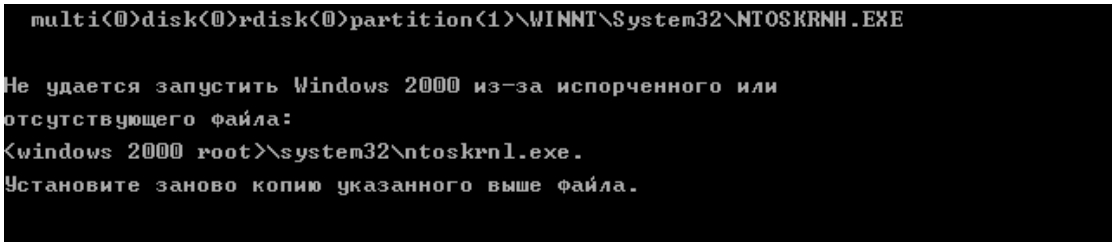


**Рисунок 1 Windows 2000 упала и не желает загружаться**

В идеале, конечно, следовало бы обратиться в ближайший сервисный центр и воздержаться от "самолечения", однако, количество _хороших_ сервисных центров можно пересчитать по пальцам одной руки, да и те завалены заказами и работают в основном на за рубеж. Остальные же, прикрываясь разнообразными лицензиями и сертификатами, не имеют никаких собственных наработок и используют утилиты массового назначения, которые пользователь может запустить и без них. Тем не менее, даже у плохого сотрудника сервисного центра есть опыт, которого у рядового пользователя нет. С другой стороны, многие виды разрушений восстанавливаются элементарно, даже без обращения к специалистам.

## *диагностика жесткого диска*

Первым делом необходимо проверить сам жесткий диск: жив ли он или уже нет? Обесточив компьютер, и выдернув PATA/SATA-шлейф, подаем питание и слушаем. Нормально работающий диск раскручивает мотор, издает характерный звук рекалибровки, после чего успокаивается. Любое другое поведение указывает на неисправность, которая может носить аппаратный (сгорела электроника), механический (навернулась механика), физический ("посыпалось" магнитное покрытие пластин) и логический (нарушилась целостность управляющей микро-ОС) характер. За исключением физической порчи блинов, все остальные повреждения поддаются восстановлению в сервисном центре, оснащенном специальном оборудованием. В домашних же условиях, без опыта и знаний, "лечение" винта гробит его окончательно.

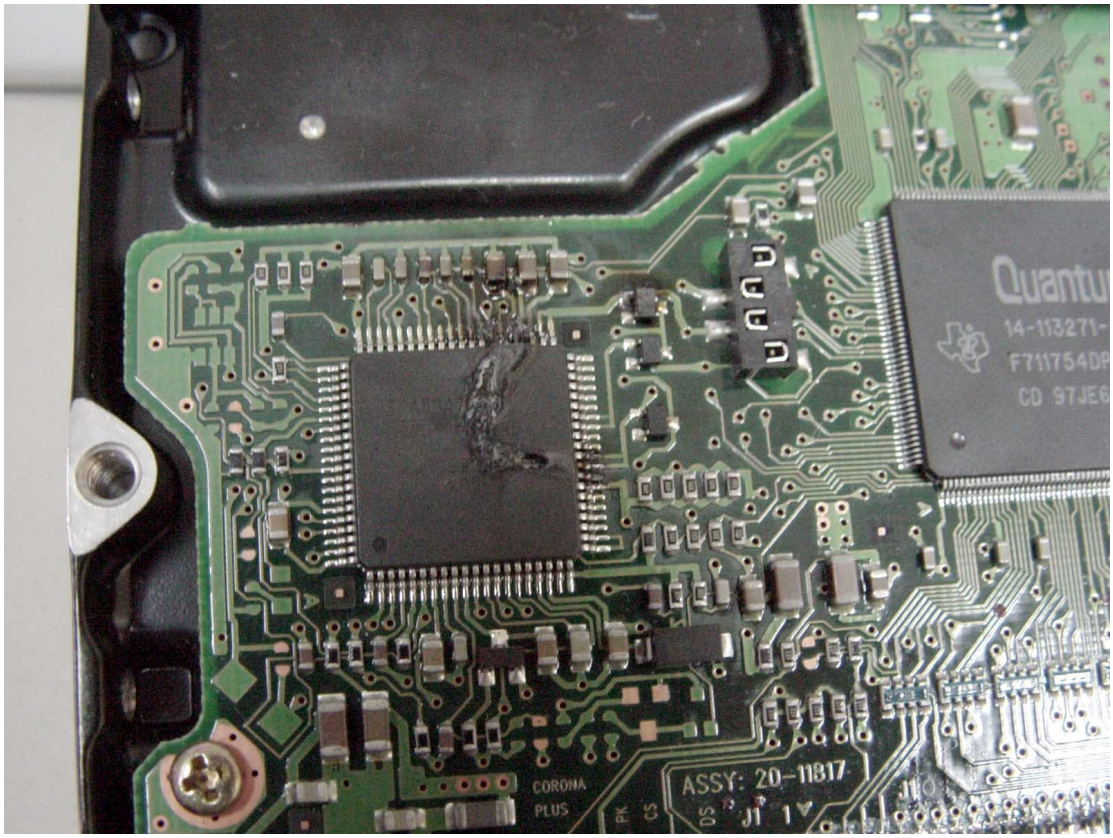


**Рисунок 2 жесткий диск с "поджаренным" чипом**

Если тест диска прошел успешно, подключаем к нему PATA/SATA шлейф, включаем компьютер и смотрим: определяется ли он в BIOS Setup или нет. Виновником может быть как сам жесткий диск, так и IDE-контроллер. На всякий случай пробуем подключить диск к другому каналу (обычно, их, как минимум, два), а еще лучше к другому компьютеру. Аналогично, проверить работоспособность IDE-контроллера можно с помощью заведомо рабочего винта.

Если жесткий диск здоров, читаем статью дальше. Если же нет — отправляем его в сервисный центр.

## *диагностика файловой системы*

Жесткий диск жив, но система не грузиться. Как так?! _Совсем_ что ли не грузиться?! Если разрушена таблица разделов или слетел загрузчик, BIOS должна заматериться об этом на английском языке. Если слетел ntldr (NT loader), поврежден реестр и т. д., система так прямо и говорит. В этом случае, файловая система с вероятностью ~90% цела, и пострадала лишь сама NT. Однако, случается так, что никаких надписей на экран не выдается и компьютер, успешно пройдя POST, впадает в завис. Причиной может быть как дефект в загрузчике/таблице разделов, так и в самом компьютере (памяти, процессоре или других компонентах). Если есть заведомо исправный компьютер — подключите винт к нему и посмотрите что будет. Ну, "что будет" сказать нетрудно: NT (в отличие от 9x) не рассчитана на смену железа и попав в неродное аппаратное окружение, скорее всего прекратит загрузку, выбросив BSOD? поэтому, действовать нужно совсем не так!

Подключаем восстанавливаемый винчестер к заведомо исправному компьютеру с установленной NT на второй IDE-канал. Загрузившись со "здоровой" NT, смотрим на подопытный диск: что там вообще есть. Если таблица разделов цела, должны появится новые логические диски. Пробуем их открыть. В лучшем случае мы увидим все свои файлы такими, какими они были до катастрофы. Или, если не все, то хотя бы часть. В большинстве случаев страдает диск C:, а остальные разделы остаются нетронутыми. Копируем все, что осталось, на резервный винчестер и пытаемся восстановить то, чего нет.

Несколько тонких нюансов. При восстановлении жестких дисков, объединенных в аппаратный RAID, подключенный к интегрированному контроллеру на материнской плате, переставлять его можно только на компьютер с аналогичным контроллером, что не всегда

просто сделать. Намного легче подключить к _этому_ _же_ компьютеру дополнительный жесткий диск, на свободный канал и установить NT/W2K/XP с лазерного диска, естественно, не забыв нажать F6 и воткнуть дискету с RAID-драйвером (иначе NT его ни за что не увидит). Изготовить такую дискету можно, загрузившись с CD-ROM-диска, поставляемого вместе с платой и следуя предложенным инструкциям. Некоторые материнские платы несут на своем борту несколько RAID-контроллеров (например, для PATA и SATA дисков) и тут главное не перепутать какой из них выбирать.

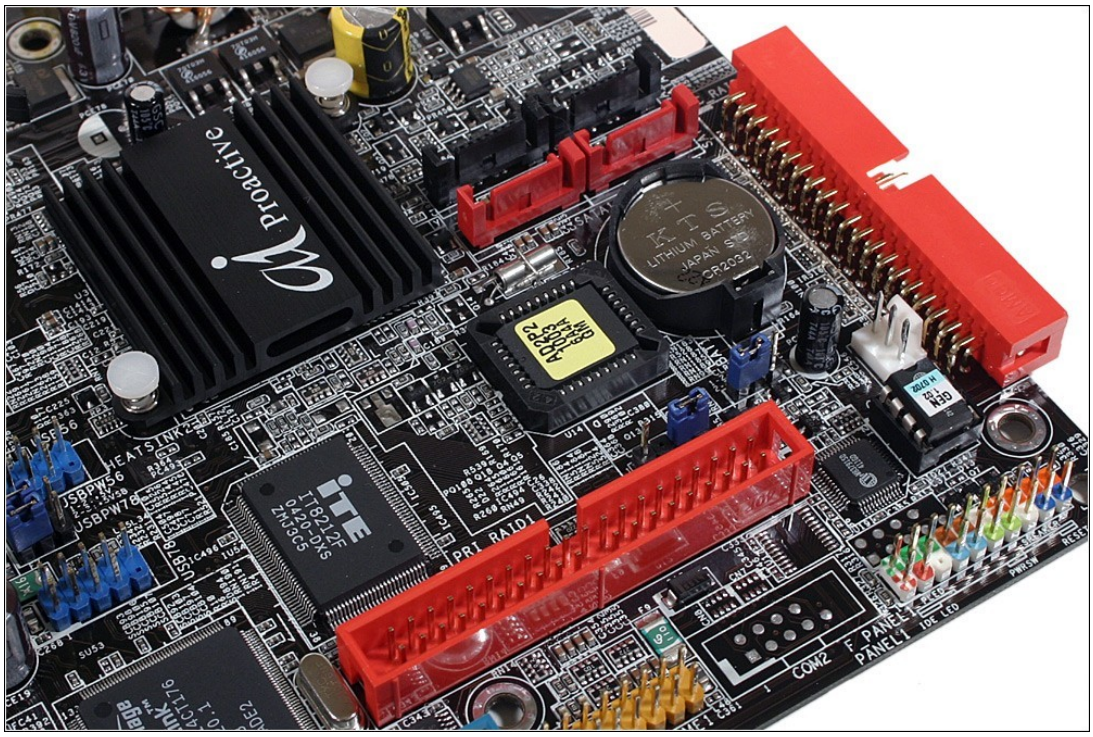


**Рисунок 3 материнская плата с интегрированным RAID-контроллером от Integrated Technology Express**

Кстати говоря, коварная (или, скорее, тупая NT) почему-то до сих пор не знает, что существует такая вещь как порядок загрузки с носителей, определяемый в BIOS. Уже лет десять как _все_ BIOS'ы позволяют грузиться с _любого_ из имеющихся жестких дисков, хоть с первого, хоть со второго, хоть с RAID'а. А вот NT самостоятельно сканирует шину, определяет порядок подключения устройств и при установке на не первый жесткий диск принудительно модифицирует загрузчик первого, записывая туда специальный код, призванный загружать систему оттуда, где она есть. Запись же на винчестер/RAID с разрушенной файловой системой/таблицей разделов носит непредсказуемый и зачастую крайне разрушительный характер. С жесткими дисками проблем нет — просто поменял шлейфы местами и все, а вот с RAID-массивами… NT вполне может увидеть RAID первым и все! Хоть ты тресни! Выход — отключаем RAID, ставим систему на новый жесткий диск (не забывая про драйвер RAID'а!), подключаем RAID и начинаем заниматься восстановлением.

С программными RAID'ми все одновременно и проще и сложнее. Данные о конфигурации дисковых массивов, созданных Windows NT 4.0 или более ранними версиями, содержится в реестре и при загрузке с другого винчестера оказываются недоступными. В Windows 2000 и более поздних версиях программные RAID-массивы создаются на базе динамических дисков, хранящих свои атрибуты в фиксированных местах диска, и потому доступных отовсюду (естественно, NT 4.0 их не увидит, но это и не страшно).

Другой подводный камень: начиная с Windows 2000 система поддерживает атрибут шифрования, позволяющий зашифровывать/расшифровывать файлы на лету без явного ввода пароля, то есть совершенно прозрачно для пользователя. На самом деле пароль (а точнее, ключ шифрования) хранится в реестре и генерируется на основе регистрационных данных пользователя случайным образом, то есть повторное создание пользователя с точно таким же именем/паролем не позволит расшифровать зашифрованные файлы, если только в нашем распоряжении нет оригинального реестра, хранящегося в файле Document-n-Setting\имя-

пользователя\NTUSER.DAT. Если он уцелел, задача восстановления зашифрованных файлов сводится к перетаскиванию его на новый жесткий диск, если же нет… Расшифровать файлы можно только тупым перебором, которым занимается множество утилит, но ни одна не дает гарантии быстрого успеха.

## >>> врезка порядок нумерации логических дисков

По умолчанию NT нумерует логические диски в следующем порядке. Букву C: получает первый раздел на первом жестком диске. Буква D: достается первому разделу _второго_ жесткого диска. Затем идут оставшиеся разделы первого жесткого диска, а за ними — второго. То есть, если мы подключаем жесткий диск (который надо восстановить) с разделами C: и D: "вторым" к диску с такими же разделами, то восстанавливаемый раздел C: следует искать на диске D:, а восстанавливаемый диск D: на диске F: (Впрочем, нумерация может быть произвольным образом изменена в "менеджере дисков").

## что делать если резервного винчестера нет

Жесткие диски сейчас дешевы как никогда, и приобрести винчестер для восстановительных целей может каждый. Правда, бывают ситуации, когда данные нужно восстановить прямо здесь и сейчас, а на часах полчетвертого ночи, за окном темень, магазины закрыты и… Или, что еще хуже, все IDE-каналы заняты программным RAID-массивом и новый диск цеплять просто некуда. В таких случаях нас выручит Windows PE, представляющая собой обыкновенный Live-CD, хорошо известный пользователям UNIX. Загрузившись с лазерного диска (не забыв нажать F6 для установки RAID-драйверов, если это необходимо), мы увидим содержимое восстанавливаемого винчестера или то, что от него осталось. Правда, в открытую продажу Windows PE так и не поступила и по официальным каналам достать ее могут либо партнеры Microsoft, либо сотрудники авторизованных сервисных центров, либо… стоп! про пиратство мы помним, но сделаем вид, что ни Осла, ни Митинского радиорынка (с кучей других ларьков) просто не существует в природе.

На самом деле, собрать Windows PE можно из обычного дистрибутива Windows 2000 с _интегрированным_ SP1 (или выше), XP или Server 2003 при помощи бесплатной утилиты Bart's PE Builder, которую можно скачать с http://www.nu2.nu/pebuilder/ и прожечь полученный образ на CD-R/CD-RW. Туда же можно закинуть и утилиты для восстановления, о которых мы поговорим в следующем разделе. PE Builder – замечательная вещь, выручающая мыщъх'а не один раз в практически безвыходных ситуациях, однако, в жизни случается всякое… Начнем с того, чтобы изготовить Windows PE необходимо иметь работающий компьютер с выходом в Сеть, а его-то в случае аварии у нас скорее всего и нет (конечно, можно и _нужно_ изготовить Windows PE заранее, но среднестатистический пользователь совершенно не заботиться о таких мелочах, увы!).


**Рисунок 4 рабочий стол Windows PE, собранной Bart's PE-Builder'ом**

В крайнем случае можно обойтись и родным дистрибутивным диском Windows 2000/XP, запустив ***консоль восстановления*** ("***recovery console***"). Это делается так: притворившись, что хотим переустановить системы, мы дожидаемся экрана с надписью "*чтобы восстановить Windows нажмите <R>*". Жмем <R> и появляется другой экран: "*для исправления установки Windows через консоль восстановления нажмите <C>; для исправления Windows с помощью операции аварийного восстановления, нажмите <R>*". Жмем <C> и попадаем в черный экран а-ля MS-DOS. Если консоль восстановления обнаружит неубитую Windows, она высветит путь к системному каталогу и предложит ввести пароль администратора. Предложение из разряда тех, от которых невозможно отказаться, но даже если мы помним пароль, не факт, что он подойдет (ведь реестр мог быть разрушен и пароль превратиться в мусор). Если же никаких следов пребывания Windows не обнаружено, нас сразу выкинут в корневой каталог диска C: (если диск C: жив) не требуя пароля.

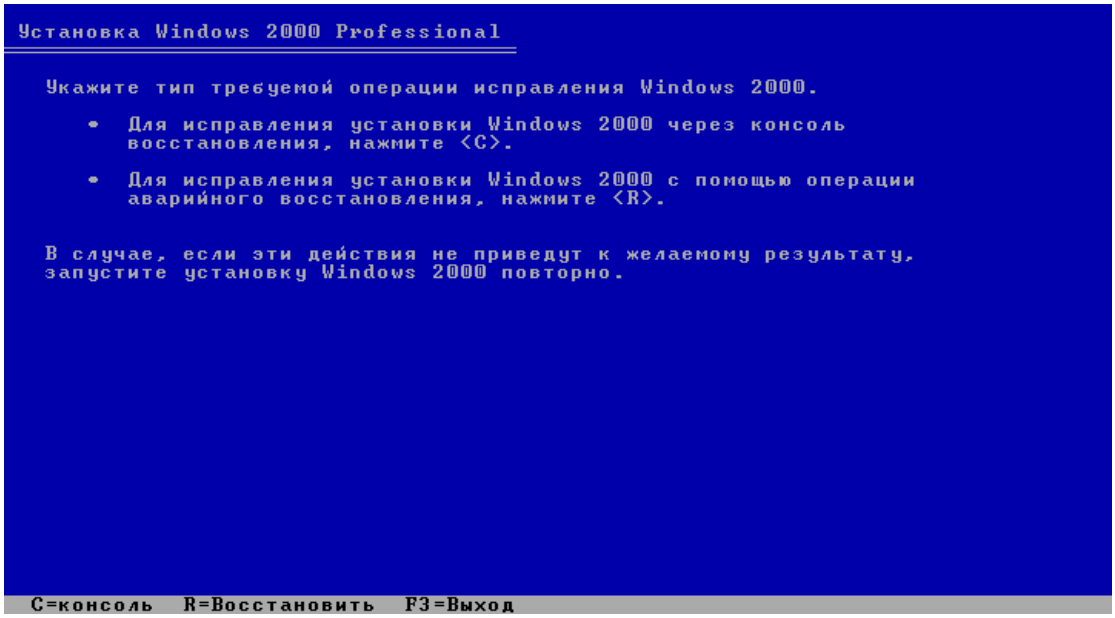


**Рисунок 5 вызов консоли восстановления**

Находясь в консоли восстановления мы можем просматривать файлы командой "`dir`" и совершать некоторые восстановительные операции встроенными командами, однако, запускать свои собственные программы, увы, невозможно, равно как и скопировать уцелевшие файлы. То есть, скопировать их, конечно, можно, но только куда? На дискету?! Да и к тому же, по умолчанию нам доступен только системный каталог (или корневой каталог диска C: если система не обнаружена). Переход в остальные каталоги (и доступ к файлам) строго запрещен хрен знает из каких соображений. К счастью, защита снимается парой магических команд: "`SET AllowAllPaths = true`" и "`SET AllowRemovableMedia = true`", после чего с диском можно делать все, что угодно.

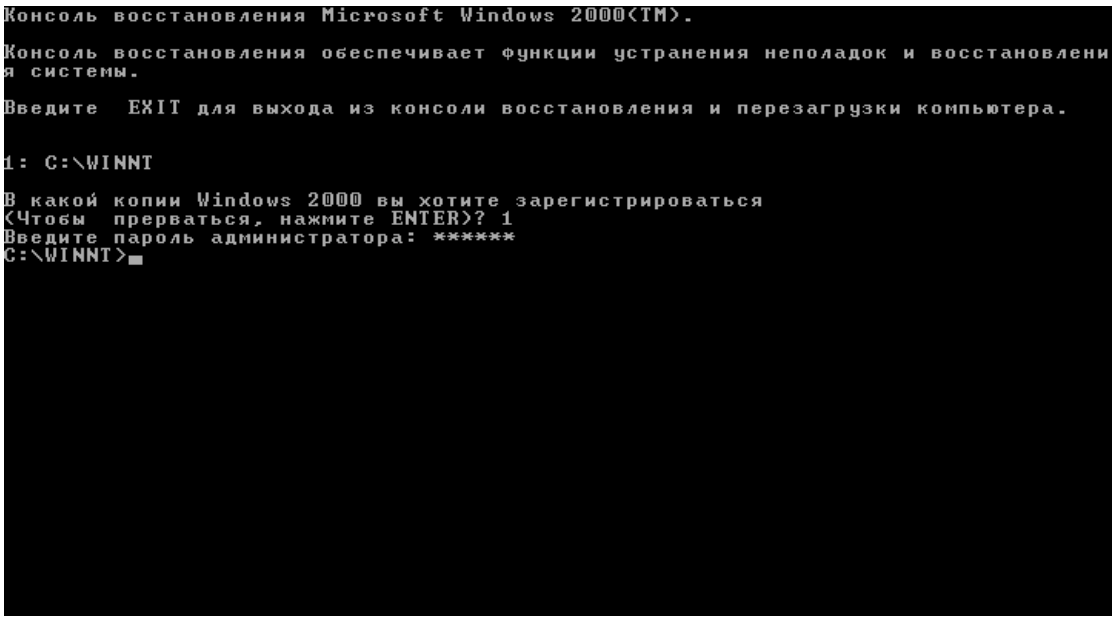


**Рисунок 6 внешний вид консоли восстановления**

## *восстановление файловой системы*

Если логические диски уцелели, но файлы на них невидны или вместо каталогов высвечивается какая-то невменяемая абракадабра, с некоторой долей риска можно запустить **`chkdsk`** из консоли восстановления, Windows PE или винчестера со здоровой NT. Несмотря на

свою кажущуюся простоту, chkdsk это довольно мощный инструмент, корректно исправляющий многие виды разрушений, но! никаких гарантий, что он не ухудшит ситуацию у нас нет, поэтому лучше оставить его каскадерам и прочим экстремалам, а самим воспользоваться *средствами* ***неразрушающего*** *восстановления* — такими, которые извлекают все уцелевшие данные, предлагая запихать их на резервный носитель (дополнительный жесткий диск, например), **не внося при этом никаких изменений в файловую систему!** Другими словами, по окончании восстановительных работ файловая система останется в том же состоянии в котором была до того, и, если результат работы утилиты нас не удовлетворит, мы можем попробовать другую, третью… пока, наконец, не найдем такую, которая решит наши проблемы.

С одной стороны это хорошо, с другой — плохо, поскольку для копирования данных требуется винчестер солидного объема, не говоря уже про необходимость повторной установки системы со всеми приложениями. Поэтому, на практике обычно действуют так: сначала запускают утилиту неразрушающего восстановления, вытягивая из диска наиболее ценные данные, а потом вызывают chkdsk — вдруг повезет и все разрушения исчезнут?

Таких утилит существует очень много, но лучшими на мой мыщъхиный взгляд являются **NtExplorer** от Runtime Software (http://www.runtime.org/) и **R-Studio** от R-TT Inc (http://www.r-tt.com/). Обе утилиты платные, однако, нашего пользователя подобные обстоятельства не смущают, тем более, что закон не запрещает держать дома Осла.


**Рисунок 7 R-Studio – одна из лучших программ автоматического восстановления**

NtExplorer – это редактор диска, поддерживающий NTFS, и ориентированный на ручную работу, однако, благодаря интуитивно-понятному интерфейсу с ним может управиться даже ребенок. В отличии от него, R-Studio представляет собой автоматизированный инструмент, осваиваемый моментально и позволяющий скопировать все уцелевшие файлы несколькими щелчками мыши. В NtExplorer'е _каждый_ файл приходится извлекать отдельно через серию операций, что, разумеется, крайне непроизводительно, однако, при некоторых разрушениях файловой системы, автоматы вроде R-Studio виснут окончательно и бесповоротно или выдают один лишь мусор, в то время как NtExplorer делает только то, что ему прикажут.

Несколько слов о внутреннем устройстве NTFS. Вся информация о файлах (и каталогах) дискового тома хранится в специальном файле, именуемом **MFT** (***M****aster* ***F****ile* ***T****able* – *Главная Файловая Таблица*), который по умолчанию хранится в начале раздела, резервируя для себя 10% от общего размера тома, однако, при недостатке места зарезервированное, но еще не занятое пространство, выделяется в "бюджет общего пользования" и тогда по мере роста MFT начинается фрагментироватся, размещаясь где попало. Это — если смотреть снаружи. Изнутри

MFT представляет собой массив **файловых записей** (**FILE RECORD**), описывающих свойства и порядок размещения на диске соответствующих им файлов. Большинство файлов описываются одной записью, некоторые (особо длинные и фрагментированные) требуют от двух и более.

Каждая файловая запись начинается с сигнатуры "`FILE*\x00`", поэтому может быть обнаружена посекторным сканированием диска даже когда таблица разделов, загрузочная запись и начало MFT полностью разрушены. Как следствие — NTFS легко выдерживает форматирование и прочие издевательства, чего нельзя сказать о FAT.

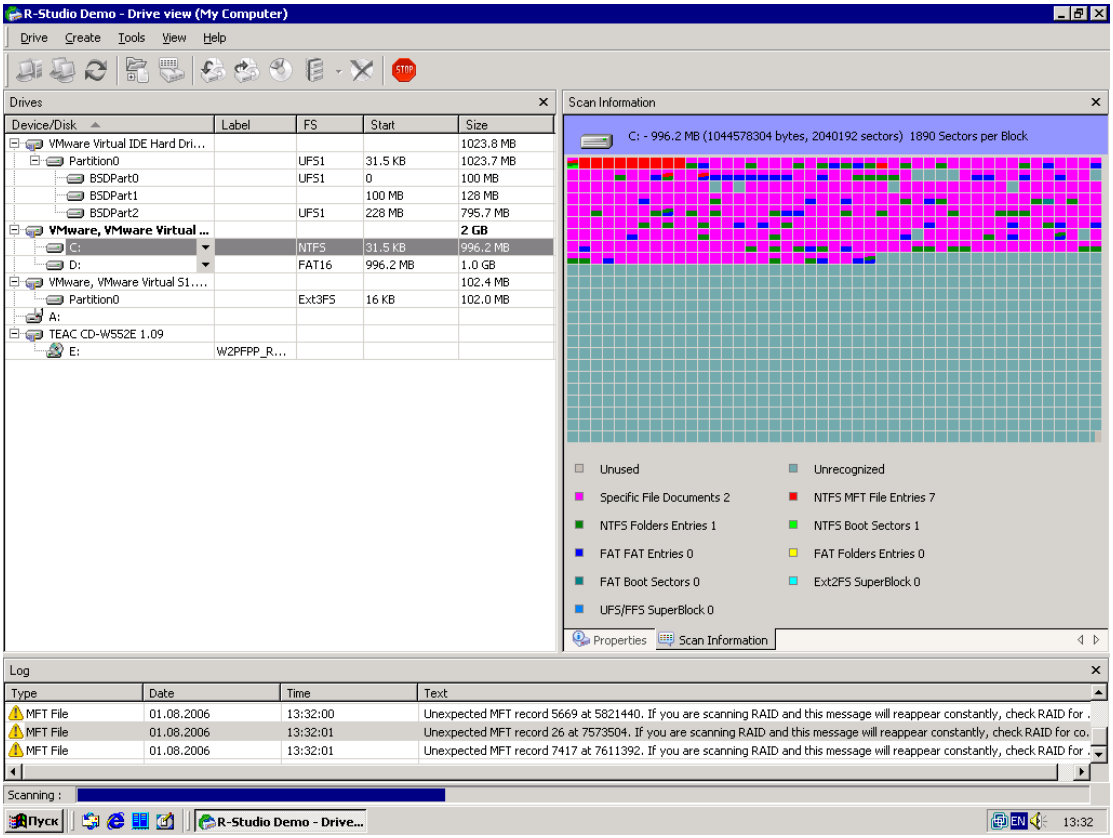


**Рисунок 8 R-Studio ищет уцелевшие файловые записи со сигнатуре "FILE*\x00"**

## *восстановление операционной системы*

Только в исключительных случаях падение NT сопровождается разрушением файловой системы (особенно на NTFS-разделах). Обычно, файловая система остается цела, а NT гробится из-за разрушения реестра некорректно работающим программным обеспечением. В стародавние времена проблема решалась установкой новой NT "поверх" упавшей, но вот сейчас… наложение сервис-паков обновляет ядро NT, делая переустановку невозможной. Инсталлятор, ругнувшись на более свежую версию, предложит либо прервать установку, либо установить систему с нуля, после чего все программы (и сервис-паки) придется переустанавливать заново, что отнимает уйму времени.

Существует несколько решений этой проблемы. Например, можно приобрести диск с уже интегрированными пакетами обновления, или воспользоваться утилитами для автоматического резервирования. Их можно разделить на два больших класса: одни (к которым принадлежит знаменитый Norton Ghost) резервируют весь системный раздел целиком, другие (типа MS Backup) сохраняют лишь системный реестр и жизненно-важные системные файлы, не трогая всего остального, если, конечно, их явно не просят о резервировании.

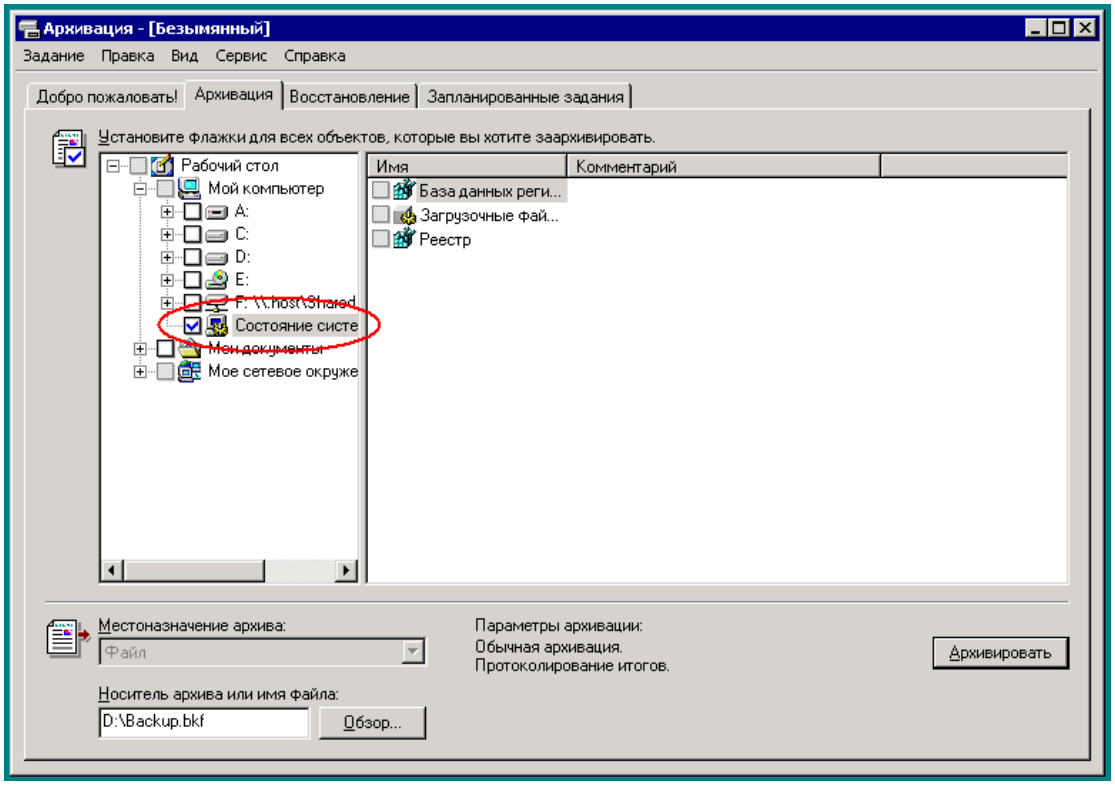


**Рисунок 9 внешний вид утилиты MS Backup**

На протяжении многих лет мыщъх пользуется штатным MS Backup'ом и остается им вполне доволен. Просто щелкаем по букве диска, выбираем "свойства", "сервис", "выполнить архивацию". В открывшемся окне выбираем вкладку "архивация", взводим галочку напротив "состояние системы", указываем путь к создаваемому файлу в окне "носитель архива или имя файла" и жмем на кнопку "архивировать". Восстановление осуществится с точностью до наоборот. В одноименной вкладке выбираем ранее созданный файл (чтобы указать путь щелкаем по левому окну правой клавишей мыши и говорим "занести файл в каталог", после чего выбираем "исходное" или "альтернативное" размещение и давим на "восстановить". Исходное размещение выбирается тогда, когда восстановление выполняется на той же самой системе, на которой оно архивировалось (то есть NT хоть и пострадала, но все-таки загружается и позволяет запускать MS Backup). В противном случае, загружаемся с другого жесткого диска/Windows PE и, выбрав "альтернативное размещение", указываем путь к папке в которой находится восстанавливаемая NT.

Сам архивный файл для надежности лучше всего держать не на винчестере, а хранить на CD-R/CR-RW, тем более что он имеет небольшой размер (порядка ~250 Мбайт).

## *заключение*

Бегло пробежавшись по основам восстановления, мы оставили за кадром столь обширный и неподъемный материал, которого хватило бы не на одну книгу или, по крайней мере, цикл статей, опубликованный мыщъхем в "системном администраторе" и теперь свободно доступный на ftp://nezumi.org.ru

## *>>>> врезка первичная диагностика аварии*

| симптом | диагноз | лекарство |
|---|---|---|
| жесткий диск не опознается BIOS'ом | отказ электроники жесткого диска | – |

| | | | |
|---|---|---|---|
| операционная система не загружается, BIOS выдает надпись "non system disk", missing operation system или что-то в этом роде | при загрузки с дискеты логические диски не видны (команда C: дает ошибку) | повреждена таблица разделов или сигнатура 55h AAh | восстановите MBR вручную или R-Studio |
| | логические разделы видны и исправны (команды C: и dir C: работают) | слетел boot и/или MBR загрузчик | запустите консоль восстановления и дайте команды FIXBMR и FIXBOOT |
| | логические разделы видны, но команда dir C: дает ошибку | поврежден boot-сектор или MTF | восстановите boot-сектор вручную или резервной копии, восстановите MFT из MFTMirr |
| операционная система начинает закружатся, но затем виснет или прерывается с сообщением об ошибке | команда dir C: выполняется нормально, chkdsk не находит ошибок | навернулась сама операционная система | переустановите операционную систему, предварительно скопировав все ценные файлы на другой носитель |
| | команда dir в одном или нескольких подкаталогах выводит мусор или показывает не все файлы | повреждена MTF или одна из ее дочерних структур | запустите Disk Explorer и прочитайте файлы из MFT напрямую в обход индексов |
| | некоторые файлы не читаются, при этом винчестер издает ритмичные скребущие звуи | физические повреждения поверхности диска | запустите утилиту восстановления жесткого диска от его производителя |
| | некоторые файлы содержат в себе фрагменты других файлов | на диске образовались пересекающиеся кластеры | запустите chkdsk |
| | свободное место на диске планомерно уменьшается без видимых причин | некоторые кластеры оказались потерянными | запустите chkdsk |